



CERT RMM for Assurance

*Transforming your
Operational Resilience Measurement
Capabilities with the
CERT® Resilience Management Model*

Software Assurance Forum
29 September 2010

Lisa Young
CERT Resilient Enterprise Management Team



Software Engineering Institute

Carnegie Mellon

© 2010 Carnegie Mellon University

Notices

NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this presentation is not intended in any way to infringe on the rights of the trademark holder.

This Presentation may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.



Software Engineering Institute

Carnegie Mellon

© 2010 Carnegie Mellon University

2



Software Engineering Institute

Carnegie Mellon

© 2006 Carnegie Mellon University

What is CERT?

- Located in the Software Engineering Institute (SEI)
 - A Federally Funded Research & Development Center (FFRDC)
 - Operated by Carnegie Mellon University (Pittsburgh, PA)
 - Separate from US-CERT
- Established in 1988 by the US Department of Defense in response to the Morris worm
- Main areas of work
 - Software Assurance
 - Secure Systems
 - Organizational Security
 - Coordinated Response
 - Education and Training



Software Engineering Institute | Carnegie Mellon

© 2010 Carnegie Mellon University

3

CERT-RMM Overview



Software Engineering Institute | Carnegie Mellon

© 2010 Carnegie Mellon University

4



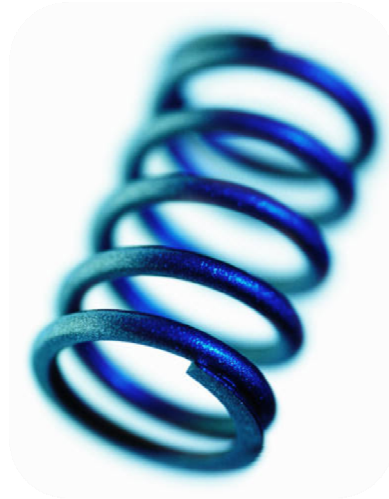
Software Engineering Institute | Carnegie Mellon

© 2006 Carnegie Mellon University

Operational resilience

Resilience: The physical property of a material when it can return to its original shape or position after deformation that does not exceed its elastic limit [wordnet.princeton.edu]

Operational resilience: The *emergent* property of an *organization* that can *continue to carry out its mission* after *disruption* that *does not exceed* its *operational* limit [CERT-RMM]



Software Engineering Institute | Carnegie Mellon

© 2010 Carnegie Mellon University

5

Operational risk & resilience

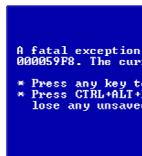
Security and business continuity are not end-states; they are continuous processes

Effective operational risk management requires these activities to work toward the same goals

Operational resilience emerges from effective **operational risk management**



Actions of
people



Systems &
technology
failures



Failed internal
processes



External events



Software Engineering Institute | Carnegie Mellon

© 2010 Carnegie Mellon University

6



Software Engineering Institute | Carnegie Mellon

© 2006 Carnegie Mellon University

What is CERT®-RMM?

CERT-RMM is a capability model for managing and improving operational resilience.

- Guides implementation and management of operational resilience activities
- Converges key operational risk management activities: security, BC/DR, and IT operations
- Defines maturity through capability levels (*like CMMI*)
- Improves confidence in how an organization responds in times of operational stress



Software Engineering Institute | Carnegie Mellon

© 2010 Carnegie Mellon University

7

Imperatives for building CERT-RMM



Tech reliance



Global economy



Open boundaries



Cultural shifts



Complexity

Increasingly complex operational environments; traditional approaches failing

Siloed nature of operational risk activities; a lack of convergence

Lack of common language or taxonomy

Overreliance on technical approaches

Lack of means to measure organizational capability

Inability to confidently predict outcomes, behaviors, and performance under times of stress



Software Engineering Institute | Carnegie Mellon

© 2010 Carnegie Mellon University

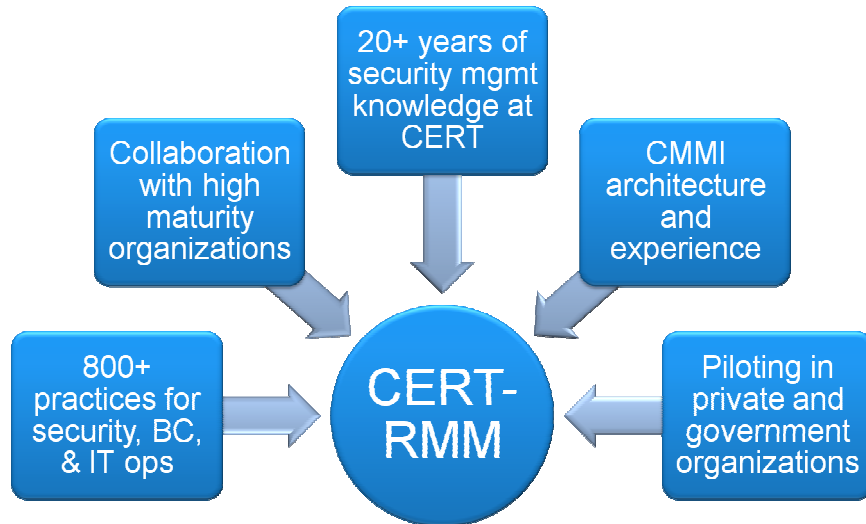
8



Software Engineering Institute | Carnegie Mellon

© 2006 Carnegie Mellon University

CERT-RMM background

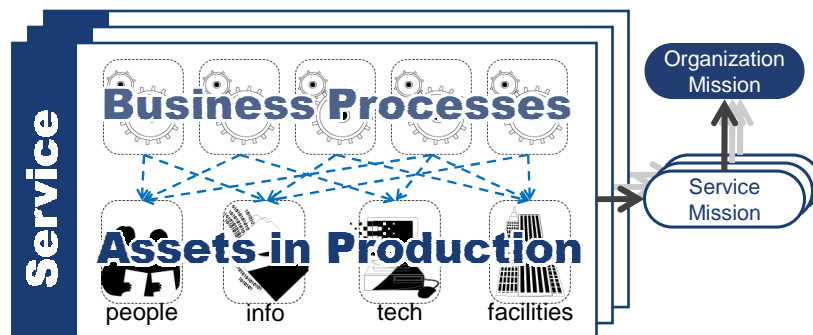


Software Engineering Institute | Carnegie Mellon

© 2010 Carnegie Mellon University

9

Organizational context



Software Engineering Institute | Carnegie Mellon

© 2010 Carnegie Mellon University

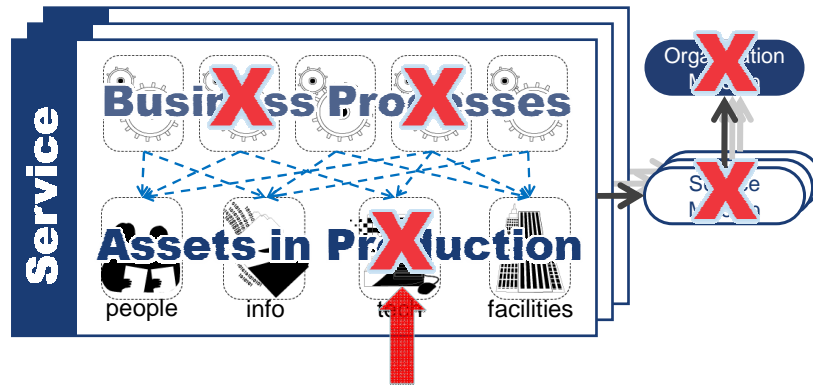
10



Software Engineering Institute | Carnegie Mellon

© 2006 Carnegie Mellon University

Organizational context - disruption



Operational risk can disrupt an asset

And lead to organizational disruption



Software Engineering Institute | Carnegie Mellon

© 2010 Carnegie Mellon University

11

CERT-RMM Architecture

How the model is put together



Software Engineering Institute | Carnegie Mellon

© 2010 Carnegie Mellon University

12

CERT-RMM: 26 process areas in 4 categories

Engineering		Operations Management	
ADM	Asset Definition and Management	AM	Access Management
CTRL	Controls Management	EC	Environmental Control
RRD	Resilience Requirements Development	EXD	External Dependencies
RRM	Resilience Requirements Management	ID	Identity Management
RTSE	Resilient Technical Solution Engineering	IMC	Incident Management & Control
SC	Service Continuity	KIM	Knowledge & Information Management
Enterprise Management		PM	People Management
COMM	Communications	TM	Technology Management
COMP	Compliance	VAR	Vulnerability Analysis & Resolution
EF	Enterprise Focus	Process Management	
FRM	Financial Resource Management	MA	Measurement and Analysis
HRM	Human Resource Management	MON	Monitoring
OTA	Organizational Training & Awareness	OPD	Organizational Process Definition
RISK	Risk Management	OPF	Organizational Process Focus

Full text of each process area is available for download at www.cert.org/resilience

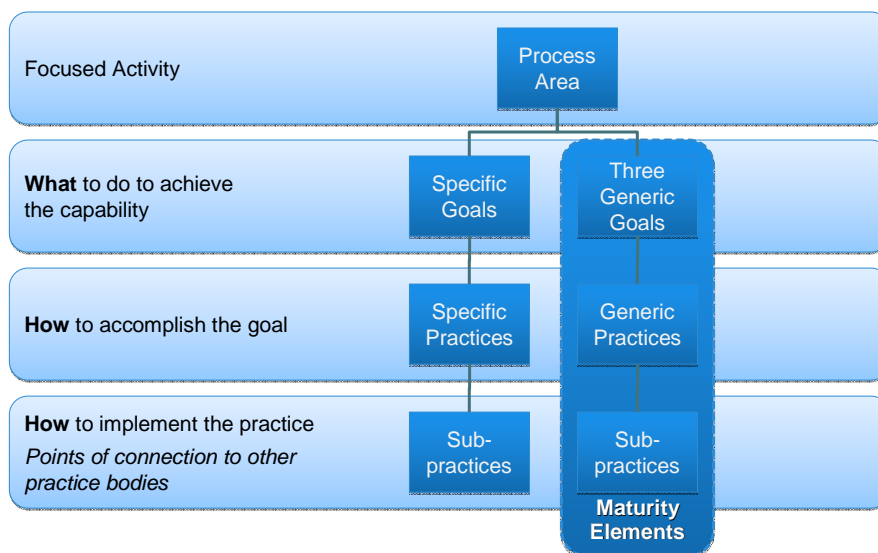


Software Engineering Institute | Carnegie Mellon

© 2010 Carnegie Mellon University

13

CERT-RMM process area architecture



Software Engineering Institute | Carnegie Mellon

© 2010 Carnegie Mellon University

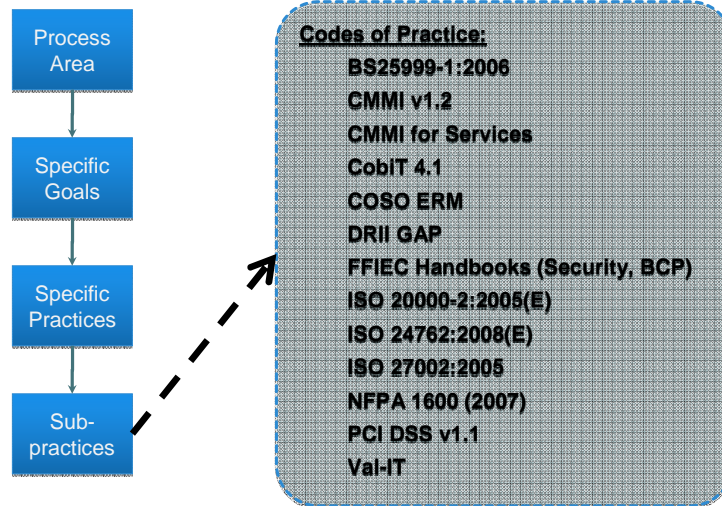
14



Software Engineering Institute | Carnegie Mellon

© 2006 Carnegie Mellon University

CERT-RMM links to codes of practice



Software Engineering Institute | Carnegie Mellon

© 2010 Carnegie Mellon University

15

Where to start

To use the model, start by selecting any number of process areas (or even parts of process areas) that align with your objectives.

Starting with 1 process area or a few specific goals is completely acceptable.

There is no requirement to use the entire model—**use whatever parts of the model make sense for your situation.**



Software Engineering Institute | Carnegie Mellon

© 2010 Carnegie Mellon University

16



Software Engineering Institute | Carnegie Mellon

© 2006 Carnegie Mellon University



Why Measure? What Should I Measure?

CERT | **Software Engineering Institute** | Carnegie Mellon

© 2010 Carnegie Mellon University 17

Why Measure?



- Demonstrate that the security program has measurable business value
- Speak to decision makers in their language
- Answer key questions
- Demonstrate that security objectives are (and continue to be) met
- Justify new investments; improve
- Help predict the future

CERT | **Software Engineering Institute** | Carnegie Mellon

© 2010 Carnegie Mellon University 18

Scope and Terminology

Measure vs. metric

- **Measure (noun):** the extent, dimensions, quantity, etc., of something, ascertained esp. by comparison with a standard: to take the measure of a thing; any standard of comparison, estimation, or judgment.
- **Metric:** pertaining to the meter or metric system; a non-negative real valued function; a system or standard of measurement; a criterion or set of criteria stated in quantifiable terms

For our efforts, metric = number; measure = number with analysis and meaning, in context. That said, our community often uses metric to mean both.



What Should I Measure?

Determine business objectives and key questions

Define the information that is needed to answer the question

- What information do you currently have?
- What additional information do you need to collect?

Qualify and quantify the information in the form of measures

Analyze the measures and report out

Quantify the value of each measure (cost/benefit)

Refine and retire measures as you go



Derive Strategic, Systemic Security Measures

Start with high-level objectives. For example, the security effort:

- 1.derives its authority from and directly traces to **organizational objectives**
- 2.satisfies security **requirements** (*) that are assigned to high-value services and their associated assets (+)
- 3.ensures that **controls** for protecting and sustaining high-value services and their associated assets operate as intended

[What do I measure to determine if these are met?]



Software Engineering Institute | CarnegieMellon

© 2010 Carnegie Mellon University

21

High-Level Security Objectives - 2

For example, the security effort:

- 4.manages **operational risks** to high-value assets that could adversely affect the operation and delivery of high-value services
- 5.ensures the **continuity of essential operations** of high-value services and their associated assets in the face of a disruptive event

[What do I measure to determine if these are met?]



Software Engineering Institute | CarnegieMellon

© 2010 Carnegie Mellon University

22



Software Engineering Institute | CarnegieMellon

© 2006 Carnegie Mellon University

Definitions - 1

Service: A set of activities that the organization carries out in the performance of a duty or in the production of a product.

High-value service: Service on which the success of the organization's mission depends.

Asset: Something of value to the organization; typically, people, information, technology, and facilities that high-value services rely on.

High-value asset: People, information, technology, or facilities on whose availability, confidentiality, integrity, and productivity a high-value service is dependent.



Definitions - 2

Protection strategy: The strategy, related controls, and activities necessary to protect an asset from undesired harm or disruptive events. The protection strategy is relative to the conditions to which the asset is subjected.

Sustainment strategy: The strategy, related controls, and activities necessary to sustain an asset (maintain in a desired operational state) when subjected to undesired harm or disruptive events. The protection strategy is relative to the consequences to which the asset is subjected.

Controls: The methods, policies, and procedures—manual or automated—that are adopted by an organization to ensure the safeguarding of assets, the accuracy and reliability of management information and financial records, the promotion of administrative efficiency, and adherence to standards.



Who, What, Where, When, Why, How

Who is the measure for? Who are the stakeholders? Who collects the measurement data?

What is being measured?

Where is the data/information stored?

When/how frequently are the measures collected?

Why is the measure important (vs. others)?

How is the data collected? How is the measure presented?
How is the measure used?



Software Engineering Institute | Carnegie Mellon

© 2010 Carnegie Mellon University

25



**CERT-RMM process areas
supporting measurement**



Software Engineering Institute | Carnegie Mellon

© 2010 Carnegie Mellon University

26



Software Engineering Institute | Carnegie Mellon

© 2006 Carnegie Mellon University

Measurement Types



Implementation

- Is this process/activity/practice being performed?

Effectiveness

- How good is the work product or outcome of the process/activity/practice? Does it achieve the intended result?

Process performance

- Is the process performing as expected? Is it efficient? Can it be planned? Is it predictive? Is it in control?



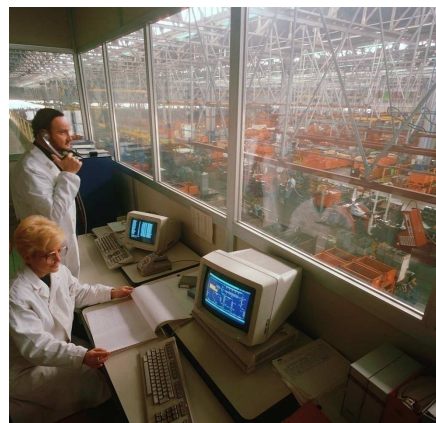
Software Engineering Institute | Carnegie Mellon

© 2010 Carnegie Mellon University

27

MON – Monitoring

Collect, record, and distribute information about the operational resilience management process to the organization on a timely basis



Software Engineering Institute | Carnegie Mellon

© 2010 Carnegie Mellon University

28



Software Engineering Institute | Carnegie Mellon

© 2006 Carnegie Mellon University

MON: Aspects of monitoring

Implicit in many CERT-RMM processes where information is needed to keep control over elements such as

- Inventories
- Communities and environments
- Artifacts and work products

The Monitoring PA elevates this activity to the enterprise for the good of all processes that need information

The monitoring process is instantiated in a program that seeks to look across operational resilience processes and provide support.



MON: Monitoring infrastructure

Supports the satisfaction of monitoring requirements and related activities

Typically a data collection and aggregation-intensive activity

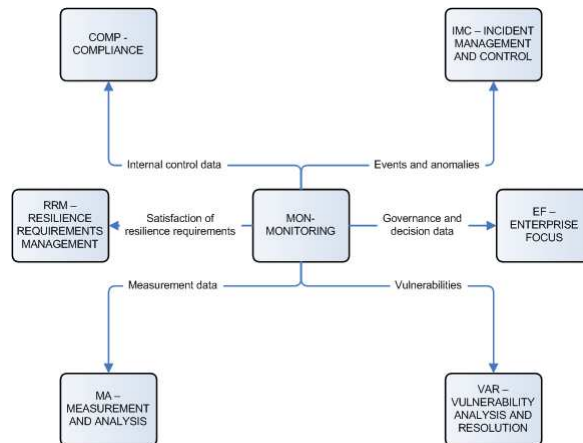
May be spread across the organization and make use of the organization's installed base of technology

Must support data quality requirements—through standards and parameters that address

- Acceptable formats and media
- Validation procedures
- Time parameters for collection of data (and “freshness”)
- Retention periods
- Regulations



Monitoring relationships



MA – Measurement and Analysis

Develop and sustain a measurement capability that is used to support management information needs for managing the operational resilience management process



MA: Overlap with MON

Primary tenet of MA is the collection of data for improving a process

Some practices in MON can satisfy practices in MA—for example, MA covers data collection and storage procedures, also important in MON.

MA is focused on the improvement process, **not** the collection of data for use in other processes—**unless** the data is being used for measurement and process improvement.



MA: Measurement objectives -1

Document the purposes for which measurement and analysis are done

Specify the kinds of actions that may be taken on the results of data analyses

May be identified at the operational unit level or the enterprise level

Sources can include

- Monitoring of resilience management process performance
- Risk conditions
- Compliance obligations
- Industry benchmarks



MA: Measurement objectives -2

May include

- “Reduce the total number of controls under management”
- “Maintain or improve supplier/customer relationships”
- “Improve uptime statistics”
- “Improve risk identification”

Once objectives are set, precise and quantifiable measures are established—can be base or derived

Example of base: Number of critical assets by category

Example of derived: Percentage of critical technology assets for which a risk analysis was conducted in last 12 months



Software Engineering Institute | Carnegie Mellon

© 2010 Carnegie Mellon University

35



CERT-RMM Resources

What's available to help people use the model



Software Engineering Institute | Carnegie Mellon

© 2010 Carnegie Mellon University

36



Software Engineering Institute | Carnegie Mellon

© 2006 Carnegie Mellon University

Resilience measurement & analysis



Area of research growing out of CERT-RMM development

Focuses on the development of adequate measures to determine transformation of operational resilience management system

Focuses on performance measurement—how well are we doing?

Includes both qualitative and quantitative measurements

Measurement users group (RMM MUG) forming—Fall 2010 opportunity to join a measurement cohort and share

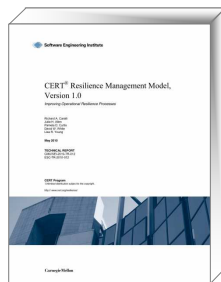


Software Engineering Institute | Carnegie Mellon

© 2010 Carnegie Mellon University

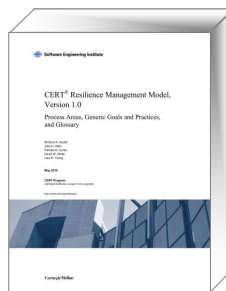
37

Download from www.cert.org/resilience



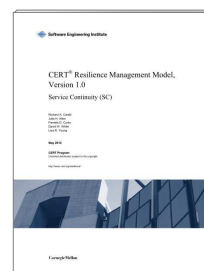
Technical Report

- Describes model structure and use
- Includes process area outlines
- 259 pages



Model v1.0

- Includes all process areas in full
- 863 pages



Process areas

- Each process area is available separately
- ~20-40 pages each



Software Engineering Institute | Carnegie Mellon

© 2010 Carnegie Mellon University

38



Software Engineering Institute | Carnegie Mellon

© 2006 Carnegie Mellon University

Questions and discussion



CERT-RMM contacts

Rich Caralli
RMM Architect and Lead Developer
rcaralli@cert.org

David White
RMM Transition Lead & Developer
dwhite@cert.org

Lisa Young
RMM Appraisal Lead & Developer
lry@cert.org

Julia Allen
RMM Developer/Measurement Team Lead
jha@sei.cmu.edu

Richard Lynch
Public Relations — All Media Inquiries
public-relations@sei.cmu.edu


Pamela Curtis
RMM Developer
pdc@cert.org

Joe McLeod
For info on working with us
jmcLeod@sei.cmu.edu



SEI Customer Relations
customer-relations@sei.cmu.edu
412-268-5800

www.cert.org/resilience






BACKUP SLIDES



  Software Engineering Institute | Carnegie Mellon

© 2010 Carnegie Mellon University 41

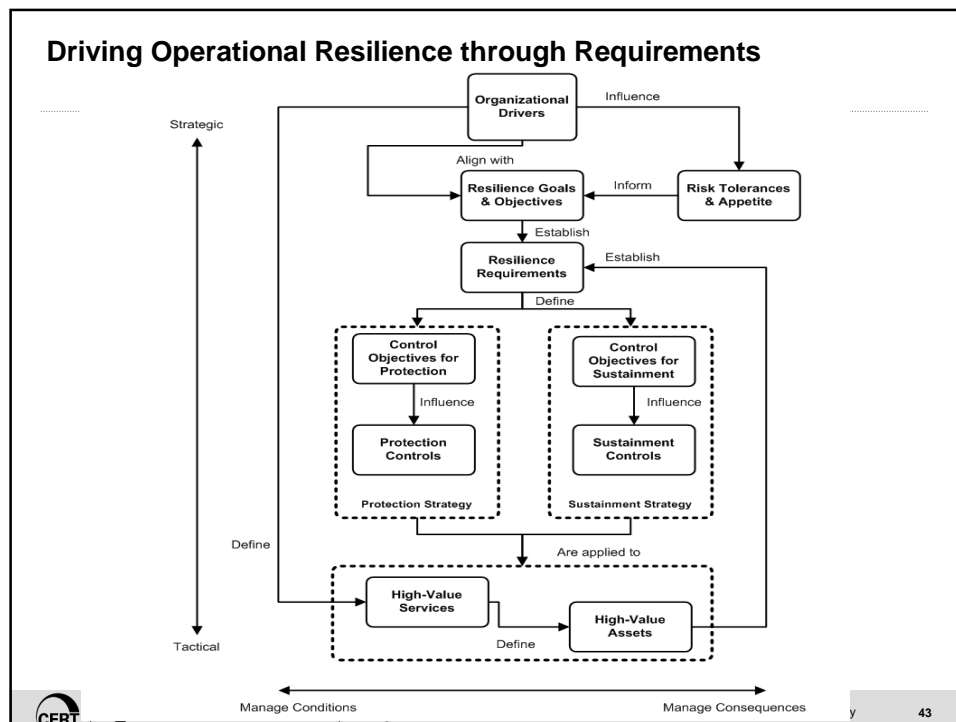


CERT-RMM for Assurance

*Focusing CERT-RMM on early lifecycle activities
for building resilience in*

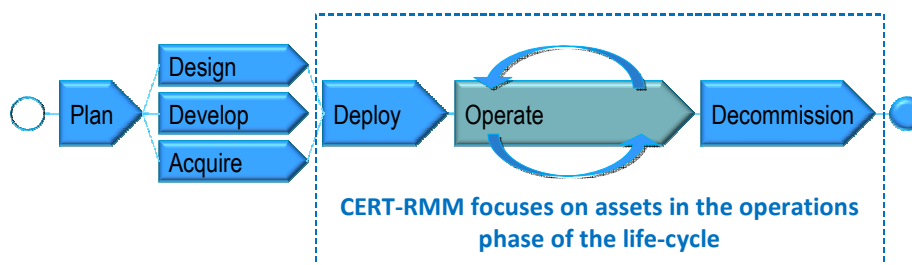
  Software Engineering Institute | Carnegie Mellon

© 2010 Carnegie Mellon University 42

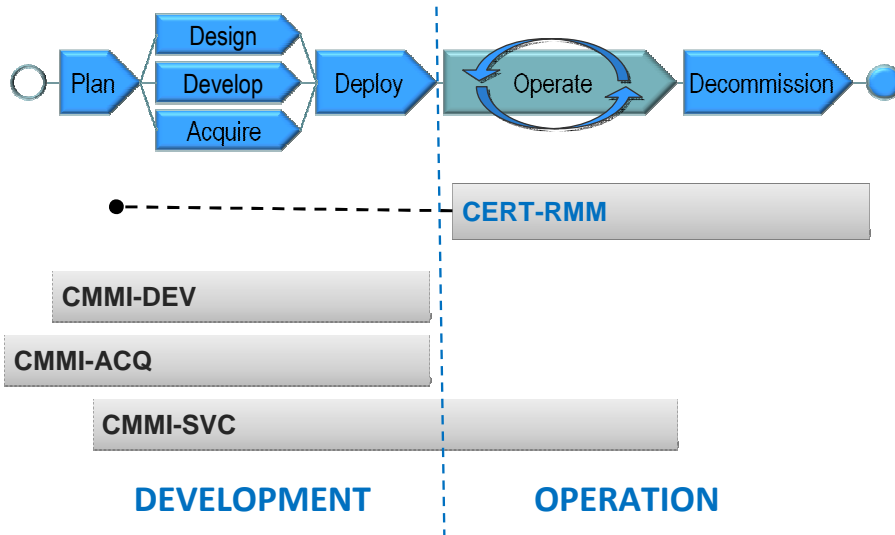


CERT-RMM in the life-cycle

Operational resilience management focuses on the deploy, operate, and decommission phases, but reaches back to development phase of lifecycle to ensure consideration of security and continuity issues prior to placing assets in production.



For comparison: CERT-RMM & CMMI



CERT-RMM assurance view

Engineering		Operations Management	
ADM	Asset Definition and Management	AM	Access Management
CTRL	Controls Management	EC	Environmental Control
RRD	Resilience Requirements Development	EXD	External Dependencies
RRM	Resilience Requirements Management	ID	Identity Management
RTSE	Resilient Technical Solution Engineering	IMC	Incident Management & Control
SC	Service Continuity	KIM	Knowledge & Information Management
Enterprise Management		PM	People Management
COMM	Communications	TM	Technology Management
COMP	Compliance	VAR	Vulnerability Analysis & Resolution
EF	Enterprise Focus	Process Management	
FRM	Financial Resource Management	MA	Measurement and Analysis
HRM	Human Resource Management	MON	Monitoring
OTA	Organizational Training & Awareness	OPD	Organizational Process Definition
RISK	Risk Management	OPF	Organizational Process Focus

26 Process Areas in 4 categories

RTSE – Resilient Technical Solution Engineering

Ensure that software and systems are developed to satisfy their resilience requirements



RTSE goals

Goal	Goal Title
RTSE:SG1	Establish guidelines for resilient technical solution development
RTSE:SG2	Develop resilient technical solution development plans
RTSE:SG3	Execute the plan



RTSE: Building in vs. bolting on

Requires organizational intervention in the development process

Extends resilience requirements to assets that are **to be developed**, not just existing assets

Creates requirements for qualities such as survivability, reliability, availability, and sustainability

Attempts to reduce the level of operational risk encountered by systems and software in production that is due to poor design and development practices

Extends across the entire software and systems lifecycle



Software Engineering Institute | Carnegie Mellon

© 2010 Carnegie Mellon University

49

RTSE: Designing and testing for resilience

Incorporates resilience-focused practices into the design and testing phases of development

Includes

- Performing resilience controls planning and design
- Incorporating resilience controls into architecture design
- Designing resilience-specific architecture
- Adopting secure coding practices
- Processes for detecting and removing defects
- Designing testing criteria to attest to asset resilience
- Testing resilience controls
- Designing service continuity plans during the development process



Software Engineering Institute | Carnegie Mellon

© 2010 Carnegie Mellon University

50



Software Engineering Institute | Carnegie Mellon

© 2006 Carnegie Mellon University

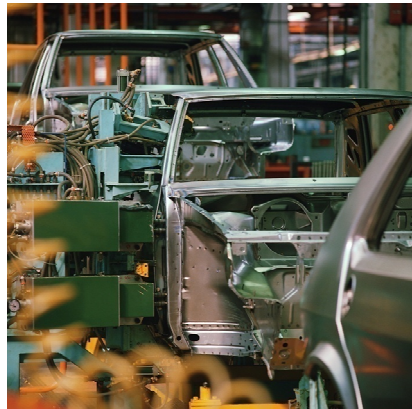
RTSE influences

- **BSIMM2** (www.bsi-mm.com)
- **Open Web Applications Security Project** (OWASP) Software Assurance Maturity Model (www.owasp.org)
- **Microsoft's Security Development Life Cycle**, v4.1 (www.microsoft.com/security/sdl/)
- **DHS Security Assurance for CMMI Process Reference Model** (buildsecurityin.us-cert.gov/swa/procwg.html)



EXD – External Dependencies Management

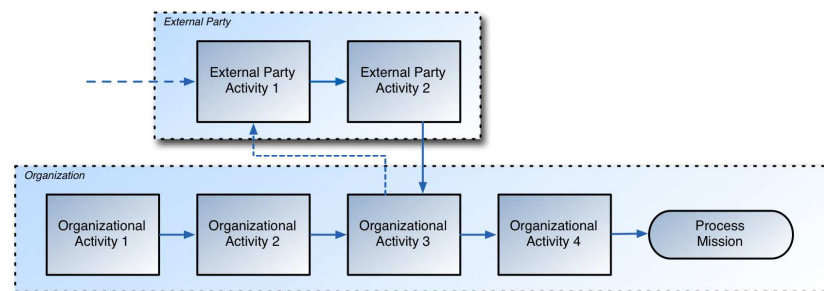
Establish and manage an appropriate level of controls to ensure the resilience of services and assets that are dependent on the actions of external entities



EXD goals

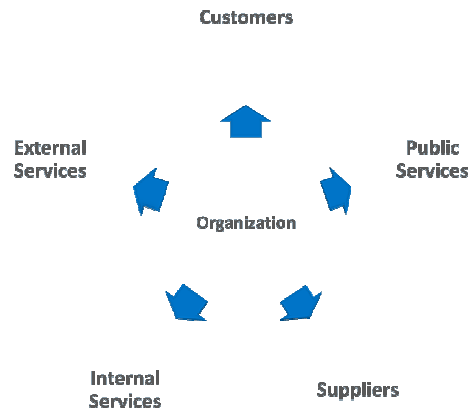
Goal	Goal Title
EXD:SG1	Identify and prioritize external dependencies
EXD:SG2	Manage risks due to external dependencies
EXD:SG3	Establish formal relationships
EXD:SG4	Manage external entity performance

EXD: Defining external dependencies



An external dependency exists when an entity that is external to the organization has access to, control of, ownership in, possession of, responsibility for (including development, operations, maintenance, or support), or other defined obligations related to one or more assets or services of the organization.

EXD: Range of dependencies to consider



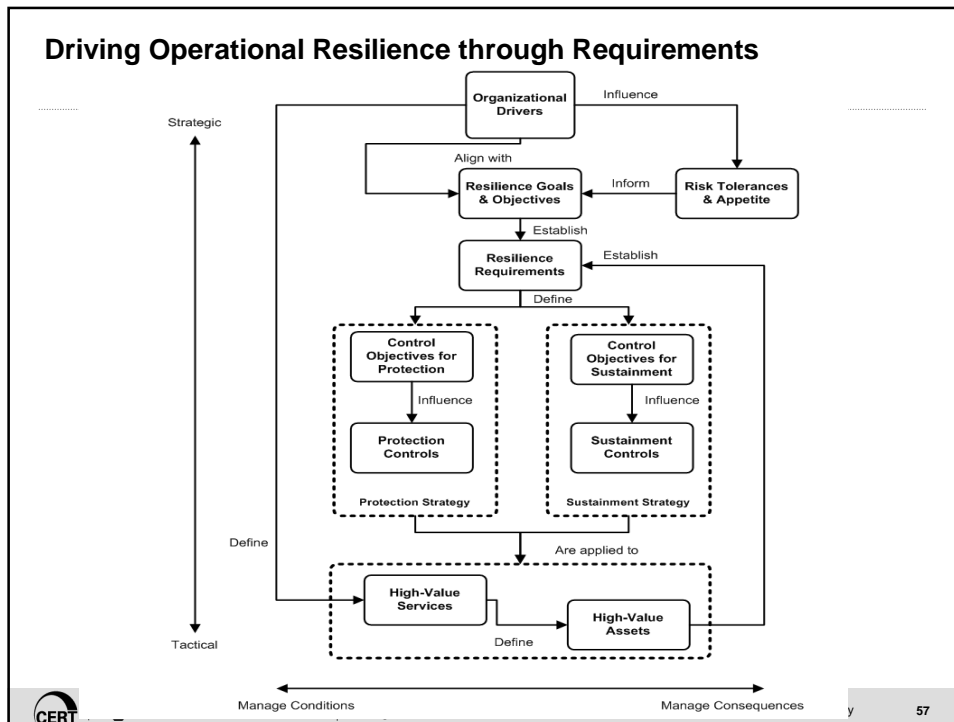
EXD: Requirements

Requirements must be established for external dependencies to protect and sustain the services that depend on the external party

- Enterprise requirements – apply to all external dependencies or to a distinct classes of external dependencies
- Specific resilience requirements – apply uniquely to an external dependency and often take the form of service level agreements

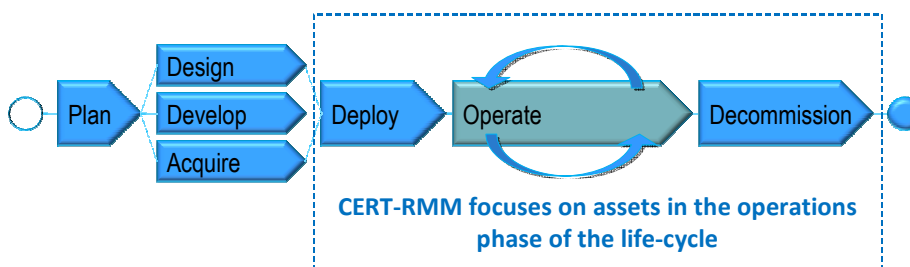
Requirements should inform the selection, negotiation of a formal agreement, and the monitoring of an external party

Unmet requirements should be treated as risks

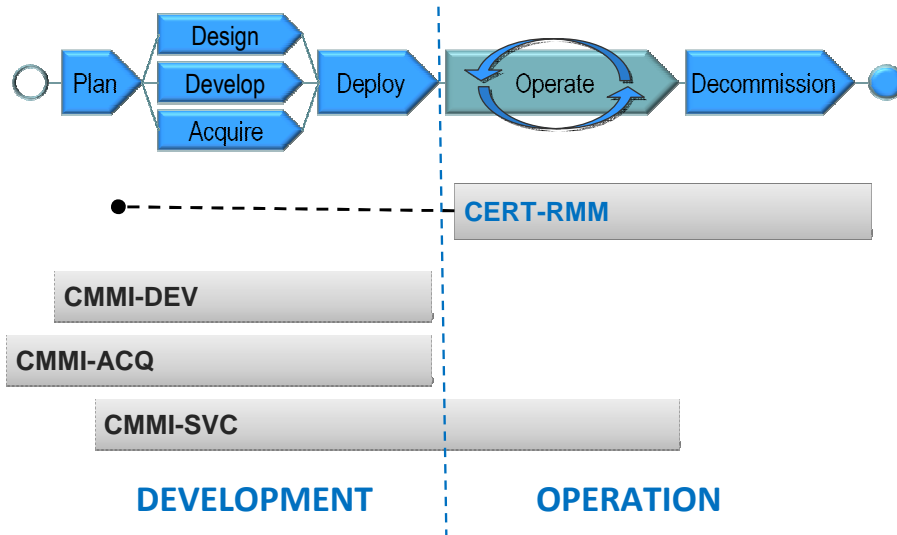


CERT-RMM in the life-cycle

Operational resilience management focuses on the deploy, operate, and decommission phases, but reaches back to development phase of lifecycle to ensure consideration of security and continuity issues prior to placing assets in production.



For comparison: CERT-RMM & CMMI



CERT-RMM assurance view

Engineering		Operations Management	
ADM	Asset Definition and Management	AM	Access Management
CTRL	Controls Management	EC	Environmental Control
RRD	Resilience Requirements Development	EXD	External Dependencies
RRM	Resilience Requirements Management	ID	Identity Management
RTSE	Resilient Technical Solution Engineering	IMC	Incident Management & Control
SC	Service Continuity	KIM	Knowledge & Information Management
Enterprise Management		PM	People Management
COMM	Communications	TM	Technology Management
COMP	Compliance	VAR	Vulnerability Analysis & Resolution
EF	Enterprise Focus	Process Management	
FRM	Financial Resource Management	MA	Measurement and Analysis
HRM	Human Resource Management	MON	Monitoring
OTA	Organizational Training & Awareness	OPD	Organizational Process Definition
RISK	Risk Management	OPF	Organizational Process Focus

26 Process Areas in 4 categories

RTSE – Resilient Technical Solution Engineering

Ensure that software and systems are developed to satisfy their resilience requirements



RTSE goals

Goal	Goal Title
RTSE:SG1	Establish guidelines for resilient technical solution development
RTSE:SG2	Develop resilient technical solution development plans
RTSE:SG3	Execute the plan



RTSE: Building in vs. bolting on

Requires organizational intervention in the development process

Extends resilience requirements to assets that are **to be developed**, not just existing assets

Creates requirements for qualities such as survivability, reliability, availability, and sustainability

Attempts to reduce the level of operational risk encountered by systems and software in production that is due to poor design and development practices

Extends across the entire software and systems lifecycle



Software Engineering Institute | Carnegie Mellon

© 2010 Carnegie Mellon University

63

RTSE: Designing and testing for resilience

Incorporates resilience-focused practices into the design and testing phases of development

Includes

- Performing resilience controls planning and design
- Incorporating resilience controls into architecture design
- Designing resilience-specific architecture
- Adopting secure coding practices
- Processes for detecting and removing defects
- Designing testing criteria to attest to asset resilience
- Testing resilience controls
- Designing service continuity plans during the development process



Software Engineering Institute | Carnegie Mellon

© 2010 Carnegie Mellon University

64



Software Engineering Institute | Carnegie Mellon

© 2006 Carnegie Mellon University

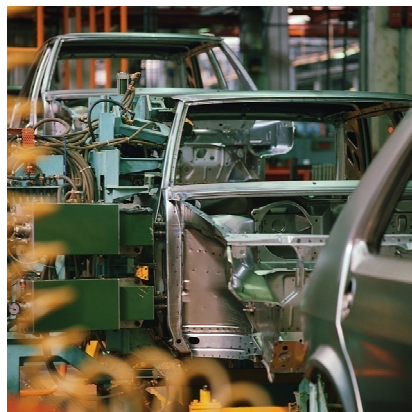
RTSE influences

- **BSIMM2** (www.bsi-mm.com)
- **Open Web Applications Security Project** (OWASP) Software Assurance Maturity Model (www.owasp.org)
- **Microsoft's Security Development Life Cycle**, v4.1 (www.microsoft.com/security/sdl/)
- **DHS Security Assurance for CMMI Process Reference Model** (buildsecurityin.us-cert.gov/swa/procwg.html)



EXD – External Dependencies Management

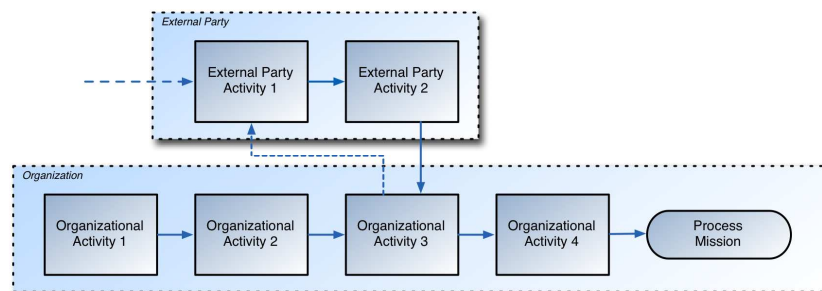
Establish and manage an appropriate level of controls to ensure the resilience of services and assets that are dependent on the actions of external entities



EXD goals

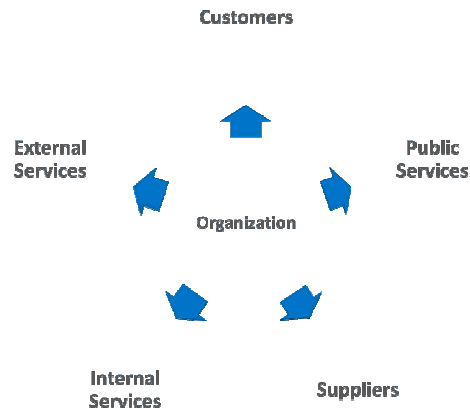
Goal	Goal Title
EXD:SG1	Identify and prioritize external dependencies
EXD:SG2	Manage risks due to external dependencies
EXD:SG3	Establish formal relationships
EXD:SG4	Manage external entity performance

EXD: Defining external dependencies



An external dependency exists when an entity that is external to the organization has access to, control of, ownership in, possession of, responsibility for (including development, operations, maintenance, or support), or other defined obligations related to one or more assets or services of the organization.

EXD: Range of dependencies to consider



EXD: Requirements

Requirements must be established for external dependencies to protect and sustain the services that depend on the external party

- Enterprise requirements – apply to all external dependencies or to a distinct classes of external dependencies
- Specific resilience requirements – apply uniquely to an external dependency and often take the form of service level agreements

Requirements should inform the selection, negotiation of a formal agreement, and the monitoring of an external party

Unmet requirements should be treated as risks